



# State of West Virginia Office of Technology

## Policy: [Acceptable Use of State-Provided Wireless Devices](#)

Issued by the CTO

---

Policy No: WVOT-PO1002

Issue Date: 01/23/07

Revised: 01/28/10

Page 1 of 14

---

### 1.0 PURPOSE (Underlined terms are defined in Section 7.0 of document)

State-provided wireless devices are made available to any employee, who by the nature of their work, must be accessible at any time of day, day of the week, or at any location.

This policy establishes a framework for procurement, possession, and appropriate use of West Virginia state-owned and/or paid [wireless](#) communication equipment and/or service within the Executive Branch.

Wireless service includes, but may not be limited to the following: voice, data, text messaging, voicemail, caller ID, call waiting, call forwarding, and three-way calling.

---

### 2.0 SCOPE

This policy applies to all [employees](#) who utilize State-owned and/or State paid wireless communication equipment and/or services, and their immediate supervisors, as well as all wireless communication service contracts entered into by the State on behalf of employees, effective as of the date of this policy.

With the rapidly changing nature of electronic media, this policy cannot provide procedures to cover every possible situation. It expresses the State of West Virginia's position and sets forth a framework to be applied to the use of electronic media and services.

This policy will supersede all other previous wireless communication policies within the Executive Branch.

---

### 3.0 RELEVANT DOCUMENTS/MATERIAL

3.1 [West Virginia Office of Technology\(WVOT\) Web Site Home Page](#)

# Policy: [Acceptable Use of State-Provided Wireless Devices](#)

## State of West Virginia Office of Technology

---

Policy No: WVOT-PO1002

Issue Date: 01.23.07

Revised: 01/28/10

Page 2 of 14

---

- 3.2 [WVOT Policies Issued by the Chief Technology Officer \(CTO\)](#)
  - 3.3 [West Virginia Code §5A-6-4a](#) – “Duties of the Chief Technology Officer Relating to Security of Government Information”
  - 3.4 WVOT-PO1001 – [WVOT Information Security policy](#)
  - 3.5 WVOT-PO1004 – [Acceptable Use of Portable Devices](#)
- 

## 4.0 POLICY

### 4.1 Conditions of Use

- 4.1.1 The State has the right to monitor and review wireless devices for operational or management purposes.
- 4.1.2 Each department is responsible for monitoring and controlling the wireless communication spending by its employees, and for keeping costs under control.
- 4.1.3 Wireless devices and service are intended to provide the means for staff to conduct State business in environments when landlines or computer networks are unavailable or impractical.
- 4.1.4 Personal use of wireless devices and service is prohibited except in certain limited and occasional circumstances that meet with the supervisor’s approval. Personal use should only occur when it does not (1) interfere with the employee’s work performance; (2) interfere with the work performance of others; (3) have undue impact on business operations; (4) incur incremental cost; or (5) violate any other provision of this policy or any other State policy, procedure, or standard. Use of wireless devices is a privilege that may be revoked at any time. (See #2, Appendix A for more information.)
- 4.1.5 The State reserves the right to address excessive personal usage and recover the cost of excessive personal usage from the user.

# Policy: [Acceptable Use of State-Provided Wireless Devices](#)

## State of West Virginia Office of Technology

---

Policy No: WVOT-PO1002

Issue Date: 01.23.07

Revised: 01/28/10

Page 3 of 14

---

4.1.6 There are examples of when limited non-business use is acceptable. They are as follows:

- 4.1.6.1 To alert household members about working late or other schedule changes;
- 4.1.6.2 To make alternative child care arrangements;
- 4.1.6.3 To talk with doctors, hospital staff, or day care providers;
- 4.1.6.4 To determine the safety of family or household members, particularly in an emergency;
- 4.1.6.5 To make funeral arrangements;
- 4.1.6.6 To reach businesses or other parties that can only be contacted during work hours; or
- 4.1.6.7 To arrange emergency repairs to vehicles or residences.

4.1.7 Examples of unacceptable use include, but are not limited to the following (For more examples of unacceptable use, see Appendix A of this document):

- 4.1.7.1 Using the wireless device while driving, without the use of a hands-free device, such as a headset, ear bud, or installation kit;
- 4.1.7.2 Using the wireless device to make 900-number and toll calls;
- 4.1.7.3 Using the wireless device to make directory assistance calls (Exceptions include emergency or unavoidable use);

# Policy: [Acceptable Use of State-Provided Wireless Devices](#)

## State of West Virginia Office of Technology

---

Policy No: WVOT-PO1002

Issue Date: 01.23.07

Revised: 01/28/10

Page 4 of 14

---

- 4.1.7.4 Purchasing and downloading games, ring tones, and/or non-business related subscription services;
  - 4.1.7.5 Using the wireless device to call State toll-free numbers (State incurs double costs); and
  - 4.1.7.6 Excessive personal use or personal use that causes additional charges on the invoice.
- 4.1.8 Employees will contact an immediate supervisor if there is doubt concerning authorization to access any State-provided IT resource, or if questions arise regarding an unacceptable use. If criminal activity is suspected or detected, reporting should occur up the supervisory or management chain without delay.
- 4.1.9 Employees must ensure that all non-business calls that would add incremental charges to the invoice are made at the employee's own expense, (e.g., charged to personal calling or credit cards, home telephones, or other non-State subsidized telephone numbers), and do not increase air time charges to the State.
- 4.1.10 Employees should have no expectation of privacy regarding their use of wireless devices. The State reserves the right to review calls, voicemail messages, text messages, etc., on all State-provided wireless devices.
- 4.1.11 The State will, consistent with applicable law and for any legitimate business reason, exercise its right to monitor, inspect, and/or review the contents of all State wireless devices at any time without the consent, presence, or knowledge of the affected employee. This may include usage, voicemail, text messages, and/or e-mail.
- 4.1.12 Employees will not knowingly or inadvertently spread computer viruses. To reduce this threat, employees must not import files from unknown or questionable sources.

# Policy: [Acceptable Use of State-Provided Wireless Devices](#)

## State of West Virginia Office of Technology

---

Policy No: WVOT-PO1002

Issue Date: 01.23.07

Revised: 01/28/10

Page 5 of 14

---

4.1.13 Employees will not be permitted to carry multiple State issued wireless communication devices if one will provide similar coverage and/or service, (ex: employees will not be able to have a Blackberry with integrated voice and data service as well as a wireless phone, or carry a pager in addition to a text message-enabled wireless phone if the geographic coverage is equivalent on both devices.)

4.1.14 Reasonable precautions should be taken to prevent equipment theft and/or vandalism. Employees must report lost or stolen wireless devices to a supervisor as soon as the loss becomes apparent.

### 4.2 Procurement

4.2.1 The State will negotiate services with several cellular providers via statewide contract(s). All cellular services must be acquired through the statewide contract(s).

4.2.1.1 Individual agencies will not be authorized to create separate contract(s) with cellular suppliers.

4.2.1.2 The State reserves the right to change service or plans at any time, for any reason, when it is in the best interest of the State.

4.2.1.3 Wireless equipment and/or services obtained independently from the statewide contract(s) will not be eligible for State reimbursement.

4.2.1.4 Wireless integrated devices, "[SmartPhones](#)" (i.e. Blackberry, Treo, and personal digital assistants [[PDA](#)] with both voice and data capabilities), or air [edge] cards are available through the statewide contract(s), and are subject to the same qualifying criteria as standard wireless devices.

# Policy: [Acceptable Use of State-Provided Wireless Devices](#)

## State of West Virginia Office of Technology

---

Policy No: WVOT-PO1002

Issue Date: 01.23.07

Revised: 01.28.10

Page 6 of 14

---

- 4.2.1.5 Agency leadership approval is required for all new orders and/or reassignments of service based on established and objective needs criteria.

---

## 5.0 STANDARD PRACTICES

### 5.1 Roles and Responsibilities

#### 5.1.1 Supervisors will be responsible for the following:

- 5.1.1.1 Approving new service;
- 5.1.1.2 Terminating or reassigning service;
- 5.1.1.3 Recovering equipment or redistributing upon separation;
- 5.1.1.4 Tracking usage and spending; and
- 5.1.1.5 Adjusting service plans (as necessary) based on usage and spending;

### 5.2 Employees will be responsible for the following:

- 5.2.1 Responsible usage to minimize spending (i.e. use land line whenever possible);
- 5.2.2 Recommending service plan adjustments based on increasing or decreasing usage requirements; and
- 5.2.3 Protection of equipment to prevent loss, unauthorized use, or disclosure of sensitive information.
- 5.2.4 Employees must report the following instances to a supervisor or designated [security contact](#):

# Policy: [Acceptable Use of State-Provided Wireless Devices](#)

## State of West Virginia Office of Technology

---

Policy No: WVOT-PO1002

Issue Date: 01.23.07

Revised: 01.28.10

Page 7 of 14

---

- Receiving or obtaining confidential information to which the employee is not entitled (Note: the owner or sender of such information must also be notified);
- Becoming aware of breaches in security; or
- Becoming aware of any inappropriate use of State-provided IT resource.

5.3 The [West Virginia Office of Technology \(WVOT\)](#), working with the Department of Administration (DOA) Purchasing Division, will be responsible for the following:

5.3.1 Negotiating contracts with suppliers; and

5.3.2 Regularly monitoring industry pricing and plan changes; and updating contracts to utilize improved plans and pricing.

5.4 Establishing a Need for Standard Wireless Service

5.4.1 Several criteria exist for establishing an approved need for standard wireless equipment and/or service (the more criteria that apply, the higher the need and likelihood of approval). This criterion includes, but may not be limited to the following:

5.4.1.1 A requirement to travel frequently on State-related business with a need beyond a calling card;

5.4.1.2 Large amounts of time spent away from the office without access to a landline;

5.4.1.3 A need for other State employees to be in constant communication with the individual;

5.4.1.4 A need for the individual to communicate frequently to support state business objectives while traveling; and/or

5.4.1.5 A consistent need for business communication outside normal business hours.

# Policy: [Acceptable Use of State-Provided Wireless Devices](#)

## State of West Virginia Office of Technology

---

Policy No: WVOT-PO1002

Issue Date: 01.23.07

Revised: 01.28.10

Page 8 of 14

---

### 6.0 ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action up to and including dismissal. Disciplinary action, if determined to be necessary, will be administered by the employing Agency and may be based on recommendations of the WVOT and the [West Virginia Division of Personnel](#), intended to address severity of the violation and the consistency of sanctions.

---

### 7.0 DEFINITIONS

- 7.1 Chief Technology Officer (CTO) – The person responsible for the State’s information resources.
- 7.2 Contractor – Anyone who has a contract with the State or one of its entities.
- 7.3 Employee – Individuals retained and authorized on a temporary or permanent basis by the State of West Virginia to perform a service. For the purposes of Information Technology and Security, the term “employee” shall include the following: contractors, subcontractors, contractors’ employees, volunteers, county health department staff, business associates, and any other persons who are determined and notified by the WVOT to be subject to this policy. This definition does not create any additional rights or duties.
- 7.4 Information Security Administrator (ISA) – The person designated by the agency head to assure the agency’s compliance with State Information Security policies and procedures. The ISA is the agency’s internal and external point of contact for all Information Security matters.
- 7.5 Information Security Liaison (ISL) - Employees assigned by the ISA to assist in the protection of information resources.

# Policy: [Acceptable Use of State-Provided Wireless Devices](#)

## State of West Virginia Office of Technology

---

Policy No: WVOT-PO1002

Issue Date: 01.23.07

Revised: 01.28.10

Page 9 of 14

---

- 7.6 Personal Digital Assistants (PDA) – A handheld device that combines computing, telephone/fax, and networking features. A typical PDA can function as a cellular phone, fax sender, and personal organizer.
  - 7.7 Security Contact – These individuals include the ISL or the ISA.
  - 7.8 SmartPhone – A wireless handheld device that supports e-mail, mobile telephone, text messaging, web browsing and other wireless information services. (ex: Blackberry, Treo, etc.)
  - 7.9 West Virginia Division of Personnel (DOP) – The Division of the Department of Administration established by WV Code § 29-6-1 et seq., which is responsible for the system of human resource management for operating agencies in the classified and classified-exempt service of West Virginia State government.
  - 7.10 West Virginia Office of Technology (WVOT) - The organization led by the State's CTO and designated to acquire, operate, and maintain the State's technology infrastructure. The WVOT is responsible for evaluating equipment and services, and reviewing information technology contracts.
  - 7.11 Wireless Device – Any device that can communicate with other devices without being physically attached to them. Most wireless devices communicate through radio frequency.
- 

### 8.0 LEGAL AUTHORITY (See West Virginia Code §5A-6-1 et seq.)

Under the provisions of West Virginia Code §5A-6-4a et seq., the [Chief Technology Officer](#) (CTO) is charged with securing State government information and the data communications infrastructure from unauthorized uses, intrusions, or other security threats. The CTO is granted both the authority and the responsibility to develop information technology policy, promulgate that policy, audit for policy compliance, and require corrective action where compliance is found to be unsatisfactory or absent.

This policy is one in a series of IT-related policies intended to define and enable the incorporation of appropriate practices into all activities using State-provided technology in the State of West Virginia.

# Policy: [Acceptable Use of State-Provided Wireless Devices](#)

## State of West Virginia Office of Technology

---

Policy No: WVOT-PO1002

Issue Date: 01.23.07

Revised: 01.28.10

Page 10 of 14

---

To the extent that there are policies in place which provide less security than this policy, they will be superseded by this policy. In instances where existing state and federal laws and regulations are more restrictive than information security policies issued by the WVOT the more restrictive provisions will prevail.

This policy is consistent with the following federal and state authorities:

- W. Va. Code § 5A-6-4a
- NIST SP 800-14 and NIST SP 800-53
- Omnibus Reconciliation Act of 1990, § 2201(c), 42 U.S.C. § 405(c)(2)(C)(viii)(I).
- Health Insurance Portability and Accountability Privacy Rule, 45 CFR 160 and 164
- Confidentiality of Substance Abuse Records, 42 U.S.C. 290dd-2; 42 CFR Part 2
- Gramm-Leach Bliley Act (GLBA), 15 U.S.C. § 6801, 16 CFR § 313
- Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*
- Driver's Privacy Protection Act, 18 U.S.C. § 2721
- Telemarketing Sales Rules, 16 CFR Part 310
- Executive Order No. 7-03 (March 25, 2003)
- Freedom of Information Act, W. Va. Code § 29B-1-1 *et seq.*
- Records Management and Preservation of Essential Records Act, W. Va. Code §§ 5A-8-21, 22
- State Health Privacy Laws, [www.wvdhhr.org/hipaa/privacy.asp](http://www.wvdhhr.org/hipaa/privacy.asp)
- Confidentiality and Disclosure of Tax Returns and Return Information, W. Va. Code § 11-10-5d
- Uniform Motor Vehicle Records Disclosure Act, W. Va. Code 17A-2A-1 to1

---

## 9.0 INDEX

### A

Acceptable Use .....	13
Appendix A.....	13
Approving New Service .....	6

### B

Blackberry .....	5, 9
------------------	------

# Policy: [Acceptable Use of State-Provided Wireless Devices](#)

## State of West Virginia Office of Technology

Policy No: WVOT-PO1002

Issue Date: 01.23.07

Revised: 01.28.10

Page 11 of 14

### *C*

Cellular Services .....	5
Chief Technology Officer .....	<i>See</i> CTO
Communication Outside of Normal Business Hours .....	7
Conditions of Use.....	2
Confidential/Sensitive Data .....	14
Contractor .....	8
CTO.....	2, 8, 9

### *D*

Disciplinary Action.....	<i>See</i> Enforcement
Downloading Software .....	4

### *E*

E-mail.....	4, 9, 14
Employee Responsibilities.....	6
Employees .....	1, 4, 5, 6, 7, 8, 14
Enforcement .....	8
Equipment Theft and/or Vandalism.....	5
Establishing a Need for Standard Wireless Service .....	7
Executive Branch .....	1, 10

### *I*

Information Disclosure .....	10
Information Resources .....	8
Information Security Administrator .....	<i>See</i> ISA
Information Security Liaison.....	<i>See</i> ISL
ISA.....	8, 9
ISL.....	8, 9
IT Policy.....	8, 9
IT Resources .....	4, 7

### *L*

Legal Authority .....	9
-----------------------	---

### *M*

Monitoring Industry Pricing and Plan Changes .....	7
Monitoring State Wireless Devices.....	4
Multiple State Issued Wireless Devices.....	5

### *N*

Negotiating Contracts with Suppliers .....	7
Non-Business Use .....	3, 4

### *P*

Pager .....	5
-------------	---

# Policy: [Acceptable Use of State-Provided Wireless Devices](#)

## State of West Virginia Office of Technology

Policy No: WVOT-PO1002

Issue Date: 01.23.07

Revised: 01.28.10

Page 12 of 14

PDA's .....	5, 8, 13
Personal Use .....	2, 4
Policy .....	2
Privacy .....	4, 14
Procurement .....	5
Protection of Equipment .....	6
Purpose .....	1
<b>R</b>	
Relevant Documents/Material .....	1
Relevant Technologies .....	13
Roles and Responsibilities .....	6
<b>S</b>	
Scope .....	1
Security Contact .....	6, 9
SmartPhone .....	5, 9
Standard Practices .....	6
State Responsibilities .....	1, 2, 4, 5, 7, 8, 9, 13
Statewide Contracts .....	5
Supervisor Responsibilities .....	6
<b>T</b>	
Terminating or Reassigning Service .....	6
Text Messages .....	4
Tracking Usage and Spending .....	6
Travel .....	7
<b>U</b>	
Unacceptable Use .....	3, 4, 13
<b>V</b>	
Viruses .....	4
Voicemail .....	1, 4
<b>W</b>	
West Virginia Code §5A-6-4a .....	2, 9
West Virginia Division of Personnel .....	8, 9
West Virginia Office of Technology .....	See WVOT
Wireless Services .....	5
Wireless Communication While Traveling .....	7
Wireless Services .....	1, 2, 4, 5, 7, 9, 12, 13
WVOT .....	1, 2, 7, 8, 9, 10, 13, 14

# **Appendix A: Technology Usage Practices**

## **State of West Virginia Office of Technology**

Policy: [Acceptable Use of State-Provided Wireless Devices](#)

Page 13 of 14

---

### **Acceptable/Unacceptable Use of State-provided Technology: Computers, Internet Access, and Wireless Devices**

The information contained within this Appendix applies to the State of West Virginia Acceptable Use of State-Provided Wireless Devices policy.

#### **Relevant Technologies**

Include, but may not be limited to the following:

- a. Personal computers;
- b. Personal Digital Assistants (PDA);
- c. Internet or Intranet;
- d. E-mail;
- e. Voice Mail;
- f. Cell phones (including camera phones and smart phones with data communications and databases);
- g. Pagers;
- h. Media including disk drives, diskette drives, optical disks (CD), tape drives, and USB drives (flash drives);
- i. Printers

#### **Unacceptable uses include, but are not limited to the following:**

- a. Any use which violates local, state, or federal laws;
- b. Any use for commercial purposes, product advertisements, or “for-profit” **personal** activity;
- c. Any use for viewing, transmitting, receiving, saving, or printing sexually explicit material;
- d. Any use for promotion of political or religious positions or causes;
- e. Any use in relation to copyright infringement;
- f. Any use in relation to participating in chain letters or unauthorized chat programs, or forwarding or responding to SPAM;
- g. Any attachment or use of devices on the State network that are not owned by the State or authorized by the WVOT;
- h. Redirecting State data to a non-State owned computing device or PDA on a routine basis, or without authorization from the CTO; or
- i. Any use in relation to downloading, attaching, changing, distributing, or installing any software or inappropriate files for non-business functions (ex: downloading MP3 files and/or broadcast audio or video files) including streaming content.

**Appendix A: Technology Usage Practices**  
**State of West Virginia Office of Technology**  
Policy: [Acceptable Use of State-Provided Wireless Devices](#)

Page 14 of 14

---

- h. Any use for promoting harassment or illegal discrimination on the basis of race, gender, national origin, age, marital status, religion, or disability;
  - i. Any use for promoting the misuse of weapons or the use of devices associated with terrorist activities;
  - j. Any use related to pyramid selling schemes, multi-marketing schemes, or fundraising for any purpose unless agency sanctioned;
  - k. Any use for dispersing data to customers or clients without authorization;
  - l. Any use in relation to placing wagers or bets;
  - m. Any use that could be reasonably considered as disruptive to another's work;
  - n. Any sending or sharing of confidential information for unauthorized purposes;
  - o. Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing.
1. Employees will not knowingly or inadvertently commit security violations. This includes doing one or more of the following:
- a. Accessing or attempting to access records within or outside the State's computer and communications facilities for which the employee is not authorized; or bypassing State security and access control systems;
  - b. Copying, disclosing, transferring, examining, re-naming, or changing information or programs belonging to another user unless given express permission to do so by the user responsible for the information or programs;
  - c. Violating the privacy of individual users by reading e-mail or private communications without legal authority, or authorization based upon documented just cause;
  - d. Misrepresenting oneself or the State of West Virginia;
  - e. Making statements about warranty, express or implied, unless it is a part of normal job duties;
  - f. Conducting any form of network monitoring, such as port scanning or packet filtering unless expressly authorized by the WVOT; or
  - g. Transmitting through the Internet confidential data, to include without limitation, credit card numbers, telephone calling cards numbers, logon passwords, and other parameters that can be used to access data without the use of encryption technology approved by the WVOT.
2. Employees are prohibited from transmitting personal information about themselves or someone else without proper authorization while using State-provided IT resources.